LLL 基底簡約と格子暗号

情報科学科　堀田　椋介　　指導教員：田坂　浩二

1　序文

量子コンピュータが実現すると素因数分解等を効率的に解くことができ、RSA 暗号等の解読が可能となってしまうことが知られている [1]。耐量子コンピュータ暗号として挙げられている暗号の 1 つである格子暗号に注目する。

定義 ([2, **定義** 1.1.1]) ベクトル空間 $\mathbb{R}^n$ の n 個の一次独立したベクトル $\{\vec{b}_1, \cdots, \vec{b}_n\}$ からなる、整数係数の線型結合全体の集合

$$\mathcal{L} = \mathcal{L}(\vec{b}_1, \cdots, \vec{b}_n) := \left\{ \sum_{i=1}^{n} a_i \vec{b}_i \in \mathbb{R}^n : a_i \in \mathbb{Z} \right\} \qquad (1)$$

を格子とする。正方行列 $B = (\vec{b}_1, \cdots, \vec{b}_n)$ を $\mathcal{L}$ の基底行列という。格子の基底行列の取り方は 1 通りではない。実際、$B, C \in M_n(\mathbb{R}$ を $\mathcal{L}$ の異なる基底行列とすると、ある $T \in GL_n\mathcal{L}$ が存在して、$C = BT$ が成立する。

主観察では，格子問題のひとつである最近ベクトル問題 (CVP) を援用した GGH 方式 (Goldreich-Goldwasser-Halevi 1997) とよばれる公開鍵暗号 の安全性について論じる。

CVP とは,「n 次元格子 $\mathcal{L}$ と，$\vec{w} \notin \mathcal{L}$ である目標ベクトル $\vec{w}$ が与えられたとき，$\vec{w}$ に最も近い格子ベクトル $\vec{v} \in \mathcal{L}$ を見つけよ」という問題で，NP 困難であることが知られる (van Emde Boas 1981)。GGH 方式では，公開鍵 B と秘密鍵 C は，同じ格子 $\mathcal{L}$ の基底行列からとってくる。適当な乱数ベクトル $\vec{e} \in \mathbb{Z}^n$ を用いて，平文 $\vec{m} \in \mathbb{Z}^n$ の暗号化は $\vec{w} = B\vec{m} + \vec{e}$ で与えられる。復号化は，$B^{-1}C\lceil C^{-1}\vec{w} \rfloor$ を計算する。ここで，$B\vec{m} \in \mathcal{L}$ なので，$\vec{e}$ の長さが小さければ $\vec{w}$ の $\mathcal{L}$ における CVP を解くことで本来なら復号化されるが，$n \geq 3$ におけるこの問題の解を与えるアルゴリズムは知られていない。ここでは “近似版” CVP を効率よく解くアルゴリズムとして知られる、Babai の最近平面アルゴリズムを用いている。今の場合，$C\lceil C^{-1}w \rfloor$ の計算の部分に用いている。これは，必ずしも $B\vec{m}$ の最近ベクトルを与えるものではないことに注意しておく。

主観察では、格子を簡約する方法の一つ、LLL 基底簡約を用いて GGH 方式の格子暗号がいかに安全なのかを検証する。

2　主観察

主観察で使う LLL 基底簡約アルゴリズムは、与えられた格子 $\mathcal{L}$ の基底行列 B に対し、各ベクトルの長さが B よりも短くなるような $\mathcal{L}$ の新たな基底行列を与える。

2 次元格子 $\mathcal{L}$ の基底行列に、LLL 基底簡約アルゴリズムを行うと、$\mathcal{L}$ の長さ最小のベクトルを含む基底行列が得られうことが分かっている。本研究では、3 次元格子の場合に LLL 基底簡約アルゴリズムを用いた GGH 方式の格子暗号の安全性の検証を行った。検証方法は以下である。

1. 秘密鍵 C を各成分が k 桁の整数からなる 3 次正方行列であって、各ベクトルのなす角 θ が $\theta \in [\frac{\pi}{2} - \frac{1}{10^2}, \frac{\pi}{2} + \frac{1}{10^2}]$ を満たすものをランダムに一つ決める。
2. 乱数ベクトル $\vec{e} \in \mathbb{Z}^3$ を、$|\vec{e}| \in [\frac{d}{2} - \frac{1}{10^2}, \frac{d}{2}]$ を満たすようにランダムに 1 つ決める。ただし、d は秘密鍵 C の各ベクトルのうち最小の長さとした。
3. 公開鍵 B:対角成分が全て 1 である 2 つの上下三角行列 $T_1, T_2 \in M_3\mathbb{Z}$ をランダムにとり、$B = CT_1T_2$ とおき、B の各成分が k'桁 $(k' > k)$ となるようにとる。
4. GGH 方式で復元可能なメッセージベクトルの有限集合 M を計算する。:$M = \{\vec{m} \in \mathbb{Z}^3 | C^{-1}\lceil C(B\vec{m} + \vec{e}\rfloor = B\vec{m}\}$
5. B に LLL 基底簡約アルゴリズムを行った基底行列 D を計算し、$M_D\{\vec{m} \in M | C^{-1}\lceil D^{-1}(B\vec{m} + \vec{e}\rfloor = B\vec{m}\}$ を求める。
6. 解読確率 $\frac{|M_D|}{|M|}$ を求める。

各ノルムの長さ $\begin{pmatrix} 108.715 \\ 68.4471 \\ 124.346 \end{pmatrix}$

\ 桁数	3 桁	4 桁	5 桁
成功率	0.736667	0.013333	0.0066667

各ノルムの長さ $\begin{pmatrix} 139.147 \\ 123.454 \\ 117.648 \end{pmatrix}$

\ 桁数	3 桁	4 桁	5 桁
成功率	0.376667	0.013333	0.003333

ここから、公開鍵の桁数を大きくしていくとほぼ解読できていないことがわかる。また、公開鍵の長さがだいたい揃っていても、解読しにくくないっていることがわかる。

3 次元での観察でここまで解読成功しないということから、LLL 簡約では到底解読できないことがわかる。

3　まとめと今後の課題

本観察では、ランダムに生成した行列を秘密鍵として、そこにユニモジュラ行列をかけ公開鍵を用意し、それを LLL 基底簡約して敵対側の鍵を作成し、解読される危険性を確認していった。主結果より、公開鍵を LLL 簡約したものでは解読できないことと、公開鍵の元となる秘密鍵の大きさがばらけているとより外部の解読が困難になることがわかった。

LLL 基底簡約では解読できないかったが、他にも様々な基底簡約方法があるので、以下のことが課題として挙げられる。

課題 1　Mathematica に搭載されている基底簡約アルゴリズムや、DeepLLL 基底簡約での観察

課題 2　暗愚解読成功しやすくなるための条件の模索

4　参考文献

[1]「量子コンピュータは公開鍵暗号にとって脅威なのか」、情報処理、47(2) 159-168 2006

[2] 青野良範・安田邪哉、「格子暗号解読のための数学的基礎」、近代科学社、2019